CLAIMS

What may be claimed is:

1. A cryptographic method, including:

receiving at a first entity a second public key M_A;

generating at least one of a first session key K_B and a first secret S_B based on the second public key M_A;

generating a first random nonce N_B;

encrypting the first random nonce N_B with at least one of the first session key K_B and the first secret S_B to obtain an encrypted random nonce;

transmitting the encrypted random nonce from the first entity;

in response to transmitting the encrypted random nonce, receiving at the first entity a data signal containing a modification of the first random nonce N_B+1; and

if the received modification of the first random nonce N_B+1 was correctly performed then performing at least one of

(i) opening a communication link at the first computer, and

(ii) generating a first initialization vector I_B.

2. The method of claim 1 which includes determining whether the received modification was correctly performed.

3. The method of claim 2 wherein determining whether the received modification was correctly performed includes checking whether the received modification of the first random

nonce N_B+1 equals a modification of the first random nonce N_B+1 as applied to the first random nonce N_B+1 by the first entity.

4. The method of claim 2 wherein determining whether the received modification was correctly performed includes checking whether the received modification of the first random nonce N_B+1 less a modification thereof as applied thereto by the first entity equals the first random nonce N_B+1.

5. The method of claim 1 wherein generating the first session key K_B includes

presenting a numeric parameter $ß_B$,

generating a first random number R_B, and

setting the first session key K_B equal to the second public key M_A raised to the exponential power of the first random number R_B, modulo parameter $ß_B$.

6. The method of claim 1 wherein generating the first secret S_B includes employing a combining function, f_B.

7. The method of claim 6 wherein employing the combining function, f_B, includes

first generating a first public key M_B, the combining function, f_B, then being employed on a first password P_B and on at least one of the second public key M_A and the first public key M_B.

8. The method of claim 7 wherein employing the combining function, f_B, on a first password P_B and on at least one of the second public key M_A and the first public key M_B includes

combining the second public key M_A and the first public key M_B with the first password P_B to produce a first result, and

hashing the first result with a secure hash.

9. The method of claim 8 wherein the secure hash is a one-way hash function.

10. The method of claim 9 wherein the one-way hash function is one of the Secure Hash Algorithm, the Message Digest 5, Snefru, Nippon Telephone and Telegraph Hash, and the Gosudarstvennyl Standard.

11. The method of claim 6 wherein employing the combining function, f_B, includes employing a plurality of combining functions to produce the first secret S_B, wherein each of the plurality of combining function produces a prior result, wherein employing a first combining function includes

generating a first public key M_B, and

employing the first combining function on a first password P_B and on at least one of the second public key M_A and the first public key M_B, and

employing each subsequent combining functions includes

employing a combining function on a prior result and on at least one of the second public key M_A, the first password P_B, and the first public key M_B, wherein the prior result produced by the last combining function is the first secret S_B.

12. The method of claim 6 wherein encrypting the first random nonce N_B includes employing a symmetrical encryption algorithm.

13. The method of claim 12, wherein the symmetrical encryption algorithm is one of the Data Encryption Standard and the block cipher CAST.

14. The method of claim 6 wherein encrypting the first random nonce N_B includes superencrypting the first random nonce N_B.

15. The method of claim 14, wherein superencrypting the first random nonce N_B includes superencrypting the first random nonce N_B with the first session key K_B and at least one of the second public key M_A, a parameter α_B, a parameter $ß_B$, a first public key M_B, the first session key K_B, a first password P_B, and the first secret S_B.

16. The method of claim 1 wherein

transmitting the encrypted random nonce from the first entity includes transmitting a first public key M_B and wherein

the received signal is encrypted based on at least one of a second session key K_B and a second secret S_B, and wherein the

second session key K_B and the second secret S_B are based on the first public key M_B.

17. The method of claim 1, wherein the signal further includes a second random nonce N_A and wherein, subsequent to generating the first initialization vector I_B, the method further including:

modifying the second random nonce N_A to obtain a modified second random nonce $N_{A_B}+1$;

encrypting the modified second random nonce $N_{A_B}+1$ with at least one of the first session key K_B and the first secret S_B to obtain an encrypted package;

transmitting the encrypted package from the first computer;

in response to transmitting the encrypted random nonce, receiving at the first computer a request to open a communication channel; and

opening the communication channel.

18. The method of claim 17 wherein encrypting the modified second random nonce $N_{A_B}+1$ includes encrypting it with the first initialization vector I_B.

19. The method of claim 17 wherein the communication channel is a two-way communication channel.

20. A computer readable storage medium containing executable computer program instructions which, when executed,

cause a first computer system to perform a cryptographic method including:

receiving at the first computer system a second public key M_A;

generating at least one of a first session key K_B and a first secret S_B based on the second public key M_A;

generating a first random nonce N_B;

encrypting the first random nonce N_B with at least one of the first session key K_B and the first secret S_B to obtain an encrypted random nonce;

transmitting the encrypted random nonce from the first computer system;

in response to transmitting the encrypted random nonce, receiving at the first computer system a data signal containing a modification of the first random nonce N_B+1; and

if the received modification of the first random nonce N_B+1 was correctly performed than performing at least one of

(i) opening a communication link at the first computer system and

(ii) generating a first initialization vector I_B.

21. A distributed readable storage medium containing executable computer program instructions which, when executed, cause a first computer system and a second computer system to perform a computer cryptographic method through a network, the method comprising:

receiving at a first computer system a second public key M_A;

generating at least one of a first session key K_B and a first secret S_B based on the second public key M_A;

generating a first random nonce N_B;

encrypting the first random nonce N_B with at least one of the first session key K_B and the first secret S_B to obtain an encrypted random nonce;

transmitting the encrypted random nonce from the first computer system to the second computer system;

in response to transmitting the encrypted random nonce, receiving at the first computer system a data signal containing a modification of the first random nonce N_B+1; and

if the received modification of the first random nonce N_B+1 was correctly performed then performing at least one of

(i) opening a communication link between the first computer system and the second computer system, and

(ii) generating a first initialization vector I_B.

22. A computer system for performing a cryptographic through a network, the computer system comprising:

a processor;

a network interface coupled to the network and coupled to the processor, the network interface receiving a page request including information on at least one of a user identification and a user password; and

a file storage device coupled to the processor, the file storage device storing copies of at least one of a user identification and a user password under control of a file management system, and wherein the processor performs a method, including

receiving at the processor a second public key M_A;

generating at least one of a first session key K_B and a first secret S_B based on the second public key M_A;

generating a first random nonce N_B;

encrypting the first random nonce N_B with at least one of the first session key K_B and the first secret S_B to obtain an encrypted random nonce;

transmitting the encrypted random nonce from the processor;

in response to transmitting the encrypted random nonce, receiving at the processor a data signal containing a modification of the first random nonce N_B+1; and

if the received modification of the first random nonce N_B+1 was correctly performed then performing at least one of

(i) opening a communication link at the processor and

(ii) generating a first initialization vector I_B.

23. The computer system of claim 22 wherein the network may be a network operating according to a hypertext transfer protocol.

24. A cryptographic method, comprising:

receiving at a first entity a second public key M_A and a second random number N_A encrypted with a second password P_A;

generating at least one of a first session key K_B and a first secret S_B based on the second public key M_A;

employing a first password P_B to retrieve the second random number N_A from the second random number N_A encrypted with the second password P_A;

modifying the second random number N_A to obtain a modified second random number N_A+1;

encrypting the modified second random number $N_{A_B}+1$ with at least one of the first session key K_B and the first secret S_B to obtain an encrypted random package;

transmitting the encrypted random package from the first entity; and

in response to transmitting the encrypted random package, at least one of

(i) receiving at the first entity a request to open a communication link, and

(ii) receiving at the first entity an encrypted data package.

25. The method of claim 24, wherein receiving the second random number N_A encrypted with the second password P_A includes receiving the second random number N_A superencrypted with the second password P_A and at least one of the second password P_A, the second public key M_A, a parameter α_A, and a parameter $ß_B$.

26. The method of claim 24 wherein generating the first session key K_B includes

presenting a numeric parameter $ß_B$,

generating a first random number R_B, and

setting the first session key K_B equal to the first public key M_A raised to the exponential power of the first random number R_B, modulo parameter $ß_B$.

27. The method of claim 24 wherein generating the first secret S_B includes employing a combining function, f_B.

28. The method of claim 27 wherein employing the combining function, f_B, includes

generating a first public key M_B, and

employing the combining function, f_B, on a first password P_B and on at least one of the second public key M_A and the first public key M_B.

29. The method of claim 28 wherein employing the combining function, f_B, on a first password P_B and on at least one of the second public key M_A and the first public key M_B includes

combining the second public key M_A and the first public key M_B with the first password P_B to produce a first result, and

hashing the first result with a secure hash.

30. The method of claim 29 wherein the secure hash is a one-way hash function.

31. The method of claim 30 wherein the one-way hash function is one of the Secure Hash Algorithm, the Message Digest 5, Snefru, Nippon Telephone and Telegraph Hash, and the Gosudarstvennyl Standard.

32. The method of claim 27 wherein employing the combining function, f_B, includes employing a plurality of combining functions to produce the first secret S_B, wherein each of the plurality of combining function produces a prior result, wherein employing a first combining function includes

generating a first public key M_B, and

employing the first combining function on a first password P_B and on at least one of the second public key M_A and the first public key M_B, and

employing each subsequent combining functions includes

employing a combining function on a prior result and on at least one of the second public key M_A, the first password P_B, and the first public key M_B, wherein the prior result produced by the last combining function is the first secret S_B.

33. The method of claim 24, wherein encrypting the modified second random number $N_{A_B}+1$ includes superencrypting the modified second random number $N_{A_B}+1$.

34. The method of claim 24, further including:

generating a first random number N_B wherein

encrypting the modified second random number $N_{AB}+1$ includes encrypting as a first data signal the first random number N_B and the modified second random number $N_{AB}+1$, and wherein

receiving at the first computer an encrypted data package includes receiving a second data signal encrypted to at least one of a second session key K_A and a second secret S_A, the second data signal including a second initialization vector I_A and a modified first random nonce N_B+1;

retrieving the modified first random nonce N_B+1 from the encrypted data package; and

if the retrieved modification of the first random nonce N_B+1 less was correctly performed then

sending from the first entity a request to open a two way communication channel.

35. The method of claim 34 which includes determining whether the retrieved modification was correctly performed.

36. The method of claim 35 wherein determining whether the retrieved modification was correctly performed includes checking whether the retrieved modification of the first random nonce N_B+1 as applied to the first random nonce N_B+1 by the first entity.

37. The method of claim 35 wherein determining whether the received modification was correctly performed includes checking whether the received modification of the first random nonce N_B+1 less a modification thereof as applied thereto by the first entity equals the first random nonce N_B+1.

38. A computer readable storage medium containing executable computer program instructions which, when executed, cause a first computer system to perform a cryptographic method including:

receiving at the first computer system a second public key M_A and a second random number N_A encrypted with a second password P_A;

generating at least one of a first session key K_B and a first secret S_B based on the second public key M_A;

employing a first password P_B to retrieve the second random number N_A from the second random number N_A encrypted with the second password P_A;

modifying the second random number N_A to obtain a modified second random number N_A+1;

encrypting the modified second random number N_A+1 with at least one of the first session key K_B and the first secret S_B to obtain an encrypted random package;

transmitting the encrypted random package from the first computer system; and

in response to transmitting the encrypted random package, at least one of

(i) receiving at the first computer system a request to open a communication link, and

(ii) receiving at the first computer system an encrypted data package.

39. A distributed readable storage medium containing executable computer program instructions which, when executed, cause a first computer system and a second computer system to perform a cryptographic method through a network, the method including:

receiving at the first computer system a second public key M_A and a second random number N_A encrypted with a second password P_A;

generating at least one of a first session key K_B and a first secret S_B based on the second public key M_A;

employing a first password P_B to retrieve the second random number N_A from the second random number N_A encrypted with the second password P_A;

modifying the second random number N_A to obtain a modified second random number N_A+1;

encrypting the modified second random number N_A+1 with at least one of the first session key K_B and the first secret S_B to obtain an encrypted random package;

transmitting the encrypted random package from the first computer system; and

in response to transmitting the encrypted random package, at least one of

(i) receiving at the first computer system a request to open a communication link, and

(ii) receiving at the first computer system an encrypted data package.

40. A computer system for performing a cryptographic method through a network, the computer system comprising:

a processor;

a network interface coupled to the network and coupled to the processor, the network interface receiving a page request including information on at least one of a user identification and a user password; and

a file storage device coupled to the processor, the file storage device storing copies of at least one of a user identification and a user password under control of a file management system, and wherein the processor performs a method, including

receiving at the processor a second public key M_A and a second random number N_A encrypted with a second password P_A;

generating at least one of a first session key K_B and a first secret S_B based on the second public key M_A;

employing a first password P_B to retrieve the second random number N_A from the second random number N_A encrypted with the second password P_A;

modifying the second random number N_A to obtain a modified second random number N_A+1;

encrypting the modified second random number N_A+1 with at least one of the first session key K_B and the first secret S_B to obtain an encrypted random package;

transmitting the encrypted random package from the processor; and

in response to transmitting the encrypted random package, at least one of

(i) receiving at the processor a request to open a communication link, and

(ii) receiving at the processor an encrypted data package.

41. The computer system of claim 40 wherein the network may be a network operating according to a hypertext transfer protocol.